United States District Court

EASTERN DISTRICT OF WISCONSIN

In the Matter of the Search of

The location sought to be searched is the residence at 1581 Oriole Way, Green Bay, Wisconsin (the "Subject Premises"). The Subject Premises is more particularly described as a two-story stand-alone residence on Oriole Way. The exterior of the lower level is brown and beige stone. The exterior of the upper level is tan vinyl siding. A mailbox is located at the end of the driveway by the street. The driveway leads to a two-car attached garage. To reach the front door from the driveway, one proceeds up approximately seven steps to the front door. The front door is brown. If one is facing the front door the number "1581" is to the right of the front door.

APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

CASE NUMBER:

I, LEE CHARTIER, being duly sworn depose and say: I am a Special Agent of the Federal Bureau of Investigation, and have reason to believe that on the premises known as

> The location sought to be searched is the residence at 1581 Oriole Way, Green Bay, Wisconsin (the "Subject Premises"). The Subject Premises is more particularly described as a two-story stand-alone residence on Oriole Way. The exterior of the lower level is brown and beige stone. The exterior of the upper level is tan vinyl siding. A mailbox is located at the end of the driveway by the street. The driveway leads to a two-car attached garage. To reach the front door from the driveway, one proceeds up approximately seven steps to the front door. The front door is brown. If one is facing the front door the number "1581" is to the right of the front door.

In the State and Eastern District of Wisconsin there is now concealed certain property, which is:

SEE ATTACHMENT A in violation of Title 18, United States Code Section 875(c)

The facts to support a finding of Probable Cause are as follows:

See attached Affidavit of Special Agent :

Continued on the attached sheet and made a part hereof. √ Yes ___ No

Signature of Affiant

Sworn to before me, and subscribed in my presence

12/2/09 12:30 pm
Date and time issued

at Green Bay, Wisconsin
City and State

James R. Sickel
Name & Title of Judicial Officer

Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

LEE CHARTIER, being duly sworn, deposes and says:

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed for approximately two years. I am currently assigned to the Joint Terrorism Task Force in the Milwaukee, Wisconsin, Division. My experience as an FBI agent includes the investigation of cases involving bomb threats and the use of computers and the Internet to commit violations of federal criminal law. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer evidence seizure and processing, and various other criminal laws and procedures. I have personally participated in the execution of more than fifteen search warrants.

2. Because this affidavit is being submitted for the limited purpose of establishing probable cause, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause to search the Subject Premises described in paragraph 4. Unless specifically indicated, all conversations and statements described in this affidavit are related in substance and in part. All times referenced in this affidavit are Eastern Standard Time.

3. There is probable cause to believe that certain property, described below, may be found within the Subject Premises described in paragraph 4. The property referred to and sought to be seized is property that constitutes evidence, fruits,

and instrumentalities of the commission of the offense of the transmission in interstate commerce of the threat to injure another, in violation of Title 18, United States Code, Section 875(c) ("the Specified Federal Offense").

4. The location sought to be searched is the residence at 1581 Oriole Way, Green Bay, Wisconsin (the "Subject Premises"). The Subject Premises is more particularly described as a two-story stand-alone residence on Oriole Way. The exterior of the lower level is brown and beige stone. The exterior of the upper level is tan vinyl siding. A mailbox is located at the end of the driveway by the street. The driveway leads to a two-car attached garage. To reach the front door from the driveway, one proceeds up approximately seven steps to the front door. The front door is brown. If one is facing the front door the number "1581" is to the right of the front door.[1] I know that FBI SA Gerald Mullen, who is also investigating this case, has driven past the residence and has taken pictures of it. I have viewed those pictures and know that the above description of the premises is accurate.

Summary of Relevant Computer and Internet Concepts

5. The Internet is a network of computers and computer networks which are connected to one another via high-speed data links and telephone lines for the purpose of sharing information. Connections between Internet computers exist across state and international borders and information sent between computers

[1]Law enforcement believes an individual who resides at the Subject Premises is committing the Specified Federal Offense. Based upon the investigation to date, law enforcement believes that individual is a minor, specifically 14.

connected to the Internet frequently crosses state and international borders, even if those computers are in the same state.

6. When an individual computer user sends e-mail or connects to another computer or computer system, including to make a telephone call, that connection is initiated at the user's computer, transmitted to the server of the Internet Service Provider ("ISP"), and eventually transmitted to its final destination. A server is a computer that is attached to a network of computers and serves many users.

7. An Internet Protocol Address ("IP address") is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots (e.g., 149.101.10.40). Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. ISP assign IP addresses to their customers' computers. An ISP might assign a different IP address to a customer each time the customer makes an Internet connection ("dynamic IP addressing"), or it might assign an IP address to a customer permanently or for a fixed period of time ("static IP addressing"). In addition, individual websites hosted on a computer server are also assigned IP addresses. The IP Address assigned to a computer connected to the Internet (whether dynamic or static) must be unique for the duration of a particular session; that is, from connection to disconnection. ISPs typically log their customers' connections, which means that the ISP can

identify which of its customers was assigned a specific IP address during a particular Internet session.

8. Log files are computer-generated files containing information about computer user activities, processes running on a computer, and the use of computer resources.

9. Based on my training and experience, I am aware that "swatting" is a malicious practice in which individuals make false emergency telephone calls to law-enforcement authorities, and describe dangerous and emergent incidents (such as hostage situations and threats of imminent violence) in an attempt to cause emergency services personnel (e.g., Special Weapons and Tactics or "SWAT" personnel) to respond in force to the address that appears to be reporting the incident. Typically, the inhabitants of the residence to which law enforcement officials respond have nothing to do with the false emergency telephone call and are completely unaware of the false emergency telephone call until the authorities arrive at the residence.

10. At a minimum, swatting leads to an improper and wasteful diversion of precious and scarce emergency personnel resources from real emergencies.

The Investigation

The Swatting Incident

11. On or about August 5, 2009, at approximately 2:12 a.m., an unknown male called the Sheriff's Department for Brown County, Wisconsin, and stated that he was a specific individual ("the Individual"), was high on drugs, and that he was going

to kill his wife and children. The sound of a weapon discharging could be heard in the background of the call. The caller also provided an address from which he purported to be calling ("the Swatted Home").

12. In response to this apparent emergency, members of the Brown County Sheriff's Department responded immediately to the Swatted Home and surrounded the Swatted Home.

13. Once at the Swatted Home, law enforcement identified the Individual, ensured that all family members were safe, and secured the Swatted Home.

14. Law enforcement then spoke with the adult individuals, including the Individual, who live in the Swatted Home. They had no knowledge of the above-described telephone call.

15. Law enforcement personnel subsequently concluded that the telephone call was a "swatting" episode.

The Investigation into the Swatting Call

16. Brown County Sheriff's Department records show an incoming call from a blocked telephone number on or about August 5, 2009 at approximately 2:12 a.m.

17. Following the incident, law-enforcement personnel served a federal grand jury subpoena on Skype Communications Sarl ("Skype"). Skype is an Internet service that permits its subscribers to place telephone calls through a computer once the computer is equipped with Skype software. In order to place a telephone call, the user must use both the Skype software and a password.

18. Skype records provided in response to the subpoena indicate that on August 5, 2009, at approximately 2:12 a.m., a party placed a telephone call to the Brown County Sheriff's Department using Skype. The records further reveal that the caller made the telephone call utilizing IP address 67.81.238.238. Skype records further reveal that the user identification "Daragosh" had been created for the Skype account used to make this telephone call.

19. Law enforcement then determined, by using a public database search, that the ISP for 67.81.238.238 at the time of the telephone call was CSC Holding, Inc., Optimum Online ("Optimum"). Law enforcement then served a federal grand jury subpoena on Optimum to determine what Optimum account was associated with IP address 67.81.238.238 at the time of the telephone call.

20. Optimum records indicate that during the time of the swatting call, IP address 67.81.238.238 was assigned to an account subscribed to by Dorinda Peck, residing at 207 Hiawatha Boulevard, Oakland, New Jersey.

21. Law enforcement recovered the audio recording of the swatting telephone call on YouTube. On the recording, numerous individuals are heard before and after the swatting call was placed to the police. The multiple voices before and after the swatting telephone call suggest that more than one individual was involved in committing the swatting telephone call. At the end of the audio recording of the swatting telephone call on YouTube, an individual asks if "Logan" sees lights. Another individual then responds in the affirmative. The first individual then instructs Logan to record videos like before.

22. Law enforcement, as part of this investigation, found a MySpace account associated with the username "Daragosh," which name is discussed above in paragraph eighteen. MySpace.com, like Facebook, is a social-networking website on which users can post personal information about themselves, post photographs, and link with other users, often referred to as "friends." The MySpace account associated the name "Logan" states that Logan resides in Green Bay, Wisconsin, and has the telephone number (920) 264-4910. Facebook records further demonstrate that "Logan" is friends with Kevin Peck, an individual who resides at the residence described above in paragraph twenty and from which the swatting telephone call initiated.

23. Subscriber records show that telephone number (920) 264-4910 is subscribed to by Amy Sabin at the Subject Premises. Law enforcement in Green Bay, Wisconsin has advised that Logan Sabin resides at the Subject Premises.

24. Law enforcement has determined that the Subject Premises is approximately .2 miles from the Swatted Home. Thus, an individual residing at the Subject Premises would easily be able to travel to the Swatted Home and record law enforcement's response to the swatting telephone call.

Threatening Call

25. A resident ("the Resident") in Wisconsin told law enforcement that on August 4, 2009, from approximately 1:05 a.m. to approximately 1:12 a.m., her residence ("the Residence") received five harassing telephone calls from unknown males. The Resident further stated that during one of the telephone calls, the caller

stated that he was going to burn the house down. In addition, during at least one call, the caller taunted the Resident that the Resident did not know where the callers were or from what numbers they were calling.

26. Skype records obtained pursuant to a federal grand jury subpoena demonstrate that Skype was used to make telephone calls to the Residence on eleven occasions on August 4, 2009, between approximately 1:05 a.m. and 1:19 a.m. Skype records demonstrate that many of these calls had no duration. Based upon my training and experience, the fact that some of the calls had no duration indicate that the call was not connected to the Residence and explain why the Resident only reported five harassing telephone calls.

27. Skype records reveal that all eleven telephone calls were placed utilizing IP address 69.23.66.141.

28. Law enforcement, using a public database, determined that on August 4, 2009, IP address 69.23.66.141 was assigned to ISP Roadrunner/Time Warner Cable.

29. Roadrunner/Time Warner Cable records, obtained pursuant to a subpoena, demonstrate that on August 4, 2009, IP address 69.23.66.141 was assigned to an account subscribed to by David Sabin, 1581 Oriole Street, Green Bay, Wisconsin, i.e. the Subject Premises.

Records Likely to be Found

30. Based on my training and experience, and on conversations that I have had with other law enforcement officers, I am familiar with the practices and methods of persons who commit swatting and false threat calls and their reliance on

computer and telephone technology to commit this criminal offense. Such individuals often create and maintain records relating to the swatting episodes, including correspondence (for example e-mails, instant messages, and chat statements) and memos, information concerning other individuals who were involved in the criminal activity, and names, addresses, and telephone numbers of potential swatting victims, sometimes stored in electronic databases on computers. Additionally, individuals engaged in swatting routinely use cellphones, Voice Over Internet Protocol ("VOIP") services (such as Skype), and voice-disguising technology to hide their identities, both during the course of the swatting incident and during any law enforcement investigation that might follow. Individuals using Skype or other VOIP services also often use Internet chat and messaging features to communicate with others while engaging in swatting and/or threatening telephone calls. Individual engaged in swatting also often keep information, including audio recordings of the telephone calls and video recordings of law enforcement responding to the telephone call, about past incidents as trophies indicating the scope of the law enforcement response that they caused.

31. I am aware based on my training and experience that users of computer equipment often create and maintain records of computer ownership and subscriptions to Internet services. Based on this information, and on the facts set forth above, there is probable cause to believe that computer-related equipment

and other items that were instrumentalities or evidence of the Specified Federal Offenses may be found at the Subject Premises.

32. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

Searches and Seizures of Computer Systems

33. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during the search of the premises, it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable

to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 160 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 80 million pages of data, which, if printed out, would result in a stack of paper over four miles high. Further, a 160 GB drive could contain as many as approximately 150 full run movies or 150,000 songs.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by

using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

34. In light of these concerns, I hereby request the Court's permission to search, copy, image and seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the image or hardware for the evidence described in Attachment A.

35. In order to search for the items described above that may be maintained in electronic media, law-enforcement personnel seek authorization to search, copy, image and seize the following items for off site review:

a. Any computer equipment and storage device capable of being used to commit, further, or store evidence of, the offense listed above;

b. Any computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including word processing

equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;

c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data;

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and

h. Files, records, programs, logs, electronic communications, scanning programs, financial records, and router configuration software.

36. Based on the foregoing, I believe that there is probable cause to believe that the items and records set forth in Attachment A will be found at the Subject Premises. In particular, such items and records would constitute evidence, contraband, and fruits of violations of the Specified Federal Offense and likewise would be instrumentalities of these violations.

ATTACHMENT A

The materials sought from the Subject Premises are:

a. Records, in whatever format, relating to swatting and/or threatening telephone calls;
b. Internet chat and instant messenger logs regarding swatting and/or threatening telephone calls;
c. Internet chat and instant messenger captures regarding swatting and/or threatening telephone calls;
d. Electronic communications regarding swatting and/or threatening telephone calls;
e. Audio and/or video recordings of swatting and/or threatening telephone calls;
f. Cell phones and other video recording devices;
g. VOIP equipment and/or VOIP technology, and/or records relating to VOIP usage;
h. User and account names and passwords for Skype or other VOIP providers;
i. Internet access logs;
j. Records of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes, books, diaries, and reference materials;
k. Records, in whatever form, pertaining to accounts held with Internet Service Providers or of Internet use;
l. Computers and peripheral equipment, including routers and modems;
m. Any computer equipment and storage devices capable of being used to commit, further or store evidence of the offense listed above;
n. Any computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;
o. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;
p. Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices or software;
q. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;

r. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data;

s. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and

t. Files, records, programs, logs, electronic communications, scanning programs, financial records, and router configuration software;

u. As used above, the terms records, documents, programs, applications or materials include records, documents, programs, applications or materials created, modified or stored in any form, including electronic media.